Cyber Threats in Hybrid Warfare: Securing the Cyber Space for the RSAF

by LTC Anthony Wong, MAJ Christopher Eng, CPT Ronald Loh Ming Yao & CPT Jeffrey Ng

Abstract:

According to the authors, as cyber attacks are gaining traction, it is essential for the Republic of Singapore Air Force (RSAF) to develop a comprehensive cyber defence strategy to ensure that our military networks are not compromised. This essay focuses on how cyber attacks have evolved over the years and how other established militaries addressed the cyber threat challenge. Drawing insights from these observations and in the face of an increasingly sophisticated cyber threat environment, the authors highlight that the RSAF would need to develop a multi-layered cyber defence strategy to guard its capabilities and operational effectiveness in peace and war.

Keywords: Warfare, Cyber Space, Cyber Attack, Evolution, Technology

INTRODUCTION

> *"Cyber attacks are integral parts of hybrid warfare... Adversaries can cripple key operating systems of target countries, steal their state and people's secrets, [and] invade the hearts and minds of people, all without stepping foot onto their soil."*
>
> *-Dr Ng Eng Hen, Minister for Defence*[1]

In the past decade, the world has progressed towards a new paradigm where cyber warfare can fundamentally alter the way future wars are fought. Cyber attacks were also waged as part of hybrid warfare in which adversaries (nation-state, state-funded or non-state actors) exploited the cyber domain to target capabilities and institutions that relied heavily on networks.[2] In addition, the evolving cyber conflicts occur not only in wartime—cyber attacks have been occurring on a persistent basis even in peacetime or during periods of low intensity conflicts.

While cyber attacks such as cyber crime and cyber espionage have dominated global news headlines, it is the growing spectrum of state-sponsored cyber attacks driven by strategic or military objectives that have become a major cause of concern for national security. Military establishments in many countries recognise the ramifications of cyber warfare. The United States (US) has declared cyber space as the fifth domain of warfare—in addition to the air, land, sea and space domains—and they have invested considerable resources in developing cyber strategies to deal with this emerging security threat.

With the increased use of cyber attacks gaining traction, it is essential for the RSAF to develop a comprehensive cyber defence strategy to ensure that our military networks are not compromised. This essay focuses on how cyber attacks have evolved over the years and how other established militaries addressed the cyber threat challenge. Drawing insights from these observations and in the face of an increasingly sophisticated cyber threat environment, the RSAF would need to develop a multi-layered cyber defence strategy to guard its capabilities and operational effectiveness in peace and war.

EVOLUTION OF THE CYBER THREAT SPECTRUM

Cyber threats have existed in various forms since the proliferation of the internet. As shown in *Figure 1*, the cyber threat spectrum could range from malicious pranks by individual hackers, profiteering through criminal activities, conduct of espionage, to nation-state cyber warfare.

In the 1990s to early 2000s, cyber attacks were traditionally conducted by hackers as a form of malicious prank or criminal groups committing cyber crime. Notable cyber threats during these early years included *SoBig*, *Bagle* and *My Doom* that affected millions of computers world-wide. These viruses or worms made malicious changes to the infected computers and generated millions of spam-messages. The more advanced viruses such as *My Doom* had the capability to control millions of computers to conduct Distributed Denial-of Service (DDoS) attacks.[4]

The potential of viruses and worms to control computers gave rise to botnets, which were used by criminal groups to commit cyber-crimes. These groups, using virus-controlled botnets, conducted DDoS attacks to extort money from businesses.[5] Botnets were also used to conduct phishing attacks with the purpose of stealing someone's identity for profiteering. According to *The Economist*, cyber-crime organisations such as the Russian Business Network sold their services to any bidders, from cyber criminals and hacktivists to organisations that wanted to steal secret data.[6]

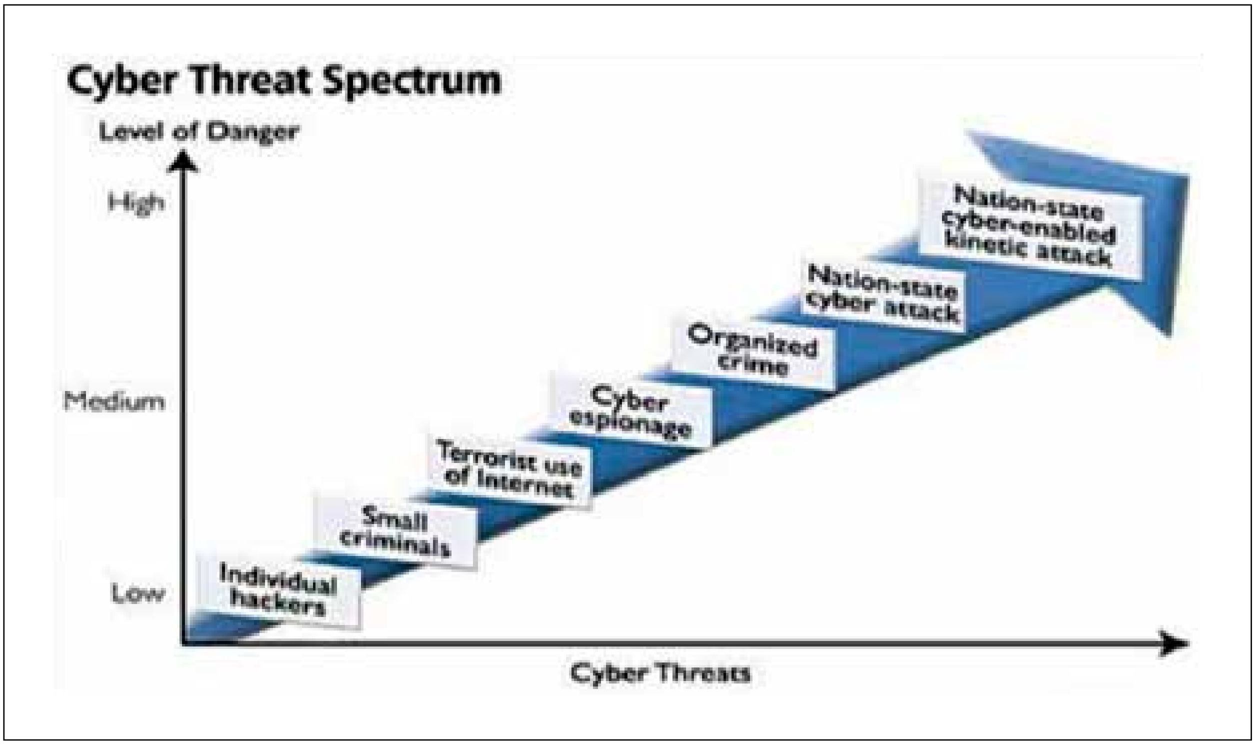


Figure 1: Spectrum of Cyber Threats.[3]

THE RISE OF STATE-LED CYBER WARFARE

Nation-state cyber attacks soon came into prominence with Russia being suspected of leveraging cyber operations to achieve its military and strategic objectives in two separate campaigns. The first incident occurred in 2007 when the Estonian government decided to remove the Bronze Soldier, a memorial commemorating the Soviet liberation of Estonia from the Nazis. Pro-Russian hacktivists, presumably under the sponsorship of the Kremlin, struck several key Estonian institutions through DDoS cyber attacks, which brought a high-tech economy and government to their knees.[7] The second operation was during the Russian-Georgian war of 2008, where cyber attacks shut down the Georgian government and local news website just before the Russian military invaded the town of Tskhinvali in Georgia, giving the Russian military total dominance over Georgia's information space.[8]

Besides Russia, Israel has also demonstrated the ability to integrate non-kinetic cyber attacks with kinetic attacks during military operations in 2007. Under Operation Orchard, the Israeli Defense Force (IDF) conducted cyber attacks on Syria's air defence systems, which allowed the Israeli Air Force to enter Syrian airspace undetected to conduct an air strike on the Syrian nuclear facility in the Deir ez-Zor region.[9]

The use of cyber attacks as a force multiplier in military operations—in the case of the Russian-Georgian war and Operation Orchard—generated intense debates amongst military strategists on cyber warfare. Advocates of cyber warfare included Lieutenant General Alexander Burutin, the Russian Deputy Chief of Staff, who predicted that future wars could be won without the physical destruction of enemy troops, "but rather by the suppression of his state and military control systems, navigation and communication systems, and also by influencing other crucial information facilities that the stability of controlling the state's economy and Armed Forces depends on."[10] Other prominent figures, such as former United States (US) Secretary of Defence Leon Panetta, also acknowledged that cyber warfare represents the battleground for the future and the potential for the next Pearl Harbour could very well be a cyber attack.[11]

The ability for nation-states to launch cyber attacks to disrupt or damage critical infrastructure through non-kinetic means was also effectively demonstrated through *Stuxnet*, which was commonly known to be developed by the United States (US) and Israel to target the Natanz nuclear enrichment plant in Iran. *Stuxnet* was designed to subvert the control systems of Natanz's Uranium centrifuges to abruptly speed up or slow down the rotor speed to the point of self-destruction while simultaneously disabling the plant's alarm systems.[12] The infiltration of *Stuxnet* into Natanz's control system demonstrated that cyber attacks could be conducted even if the targeted systems were 'off-the-grid'.

As the world came to terms with *Stuxnet*, Israel was suspected to have developed *Flame*, a highly sophisticated espionage programme that infected mainly Middle-Eastern countries, especially Iran.[13] In 2011, a worm similar to *Stuxnet*, codenamed *Duqu*, was also discovered. *Duqu's* purpose was to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, and thereby enable its designer to conduct a future attack more easily against another third party.[14]

STUXNET AND BEYOND: THE RISE OF ADVANCED PERSISTENT THREATS

The development of highly sophisticated malware such as *Stuxnet*, *Flame* and *Duqu* represented a key shift from traditional DDoS and mass phishing cyber attacks towards Advanced Persistent Threats (APTs) in cyber warfare. According to the National Institute of Standards and Technology, APT is "an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors."[15] APT attacks are typically highly targeted with a clear objective, which could range from cyber-espionage to cyber attacks on critical infrastructures, operating systems or organisations. Given the sophistication of APT attacks and the resources required to carry out these attacks, actors behind APT are usually state-sponsored and may operate in tandem with military or state intelligence.[16]

Evidence suggests that current cyber security mechanisms are often ineffective in dealing with APT, which often uses sophisticated means to evade cyber detection. Research showed that the average number of days from infection to identification of the APT was 416 days.[17] For example, a long-running APT codenamed Operation Dust Storm has been active since 2010, but the existence and extent of damage of this APT was only recently revealed. According to security firm Cylance, the hackers behind this operation targeted various organisations in Asia, the US and Europe from 2010 to 2015. These hackers used various means to conduct their cyber attacks, ranging from launching watering holes and phishing attacks to remote access Trojans and zero-day exploits. In 2015, these hackers also leveraged Android backdoors (instead of Windows backdoors) to deliver a strain of malware dubbed 'Misdat', which would allow hackers to gain unauthorised access and control of the infected computer systems. Given that the group was well-organised and well-funded, Cylance researchers believed that this operation involved a nation-state actor.[18]

CHALLENGES IN CYBER DEFENCE

The evolving nature of these highly sophisticated cyber threats highlights three key challenges in cyber defence. First, while passive cyber defences measures can prevent low-level attacks, it is no longer effective in countering sophisticated cyber attacks. APTs are designed to target system vulnerabilities or behaviour analysed through intelligence gathering. They are built to circumvent existing network defences, evade detection, and wait to be triggered before delivering their malicious code to infect the targeted system.

Second, it is easier for a cyber attacker to carry out an attack than it is to defend against it. It is difficult for cyber defence methods to completely eliminate any intrusions as new vulnerabilities in operating software, hardware, and network architecture are constantly being identified. In addition, organisations may not have any indications that their systems have been compromised until the installed malware is triggered to carry out the attack. Therefore, part of an effective cyber defence strategy is to determine a baseline capability to ensure operational continuity. It is also important to strengthen the resilience of networked systems and prevent a steep capability drop after suffering a cyber attack. Thereafter, action plans must kick in to recover to full capability.

Third, the human factor is usually the weakest link in any cyber defence. Any personnel could be targeted for spear phishing and these personnel could inadvertently transfer malware into their own system. Furthermore, an insider who fails to adhere to the established cyber security practices risks introducing malware into even a closed system. The most prominent example would be the *Stuxnet* infection, which was introduced into Natanz's closed network through a USB thumb drive by an employee working in engineering.

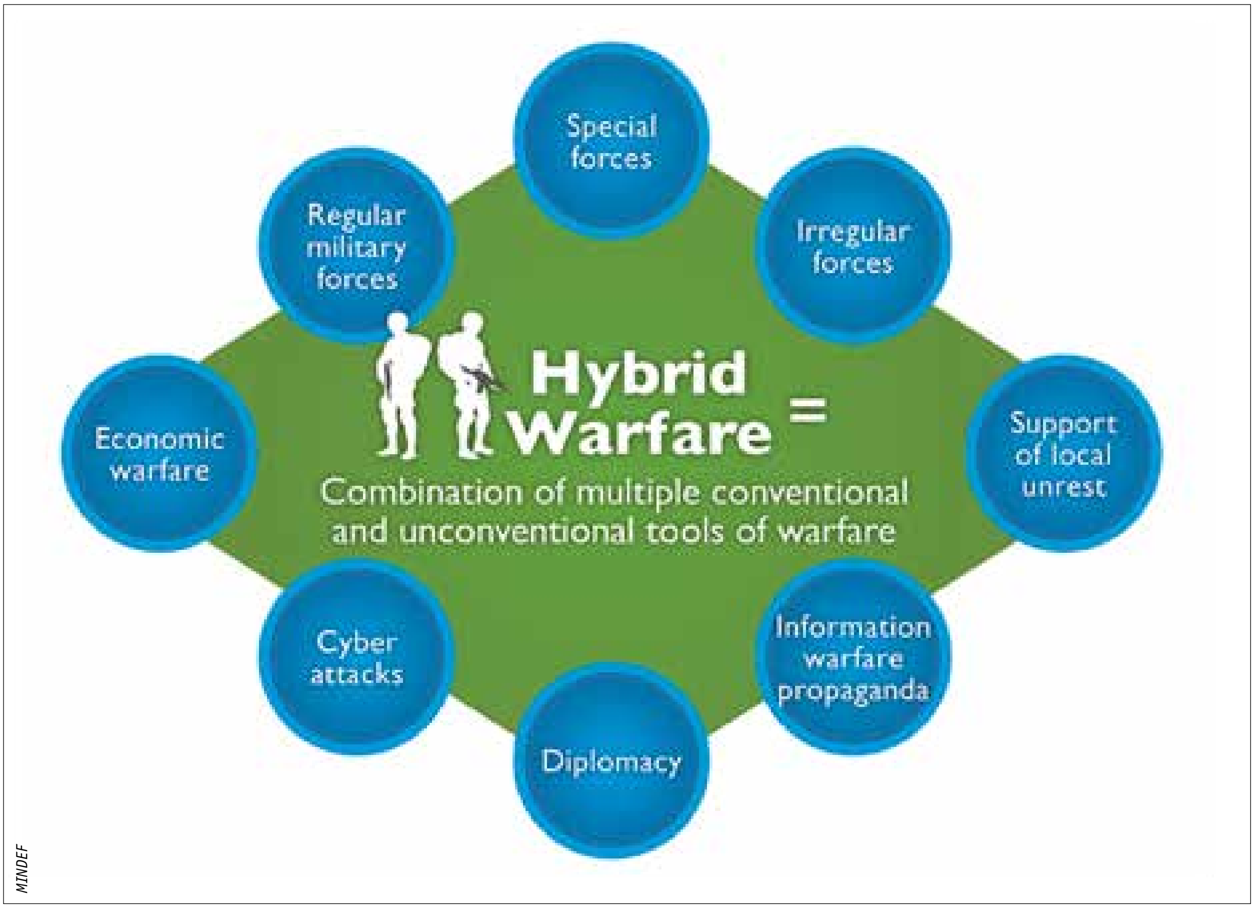
CYBER DEFENCE STRATEGY IN THE EVOLVING CYBER THREAT ENVIRONMENT

Given the rise in advanced cyber attacks and the risks it poses to a state's national security, militaries around the world have evolved their cyber defence strategy to address the increasing threats.

US Cyber Strategy

For the US Department of Defence (DoD), the compromise of its classified military networks in 2008 was a wake-up call for the Pentagon to develop a comprehensive cyber defence strategy to counter cyber attacks. The 2008 intrusion was not the only successful cyber attack. According to William Lynn, the then-US Deputy Secretary of Defence, adversaries of the US have also "acquired thousands of files from US networks and from networks of US allies and industry partners, including weapons blueprints, operational plans and surveillance data."[19]

Recognising that passive cyber defence approaches such as firewalls, patching of security vulnerabilities and virus and threat detections are no longer adequate to counter APT, the US developed the concept of active cyber defence in 2010 to complement its passive cyber defence approach. The US DoD



MINDEF

Figure 2: Dr Ng Eng Hen cited the recent unrest in Ukraine as an example of hybrid warfare, where subversion and subterfuge were conducted both through agents on the ground as well as through disinformation on social media

defines active cyber defence as its "synchronised, real-time capability to discover, detect, analyse and mitigate threats and vulnerabilities... It operates at network speed by using sensors, software and intelligence to detect and stop malicious activity before it can affect US DoD networks and systems."[20] Lynn highlighted that the active cyber defence approach would allow the Pentagon to build "layered and robust defences around military networks."[21]

Given the rise in advanced cyber attacks and the risks it poses to a state's national security, militaries around the world have evolved their cyber defence strategy to address the increasing threats.

As part of developing a comprehensive cyber defence approach, the Pentagon also inaugurated the US Cyber Command to "integrate cyber defence operations across the military."[22] The consolidation of cyber defence capabilities under one roof enabled the US Cyber Command to leverage on the government's intelligence capabilities to provide highly specialised active defences, such as detection and forensics, deception and attack termination.

Israel's Cyber Strategy

Similar to the US, Israel has also been a prime target for cyber attacks. During Operation Protective Edge in 2014, Israel faced large-scale cyber attacks on its civilian communications infrastructure via multiple DDoS and Domain Name System (DNS) attacks. The IDF's military communication networks were also targeted as part of the cyber attacks.[23] Senior Israeli security sources claimed that the attacks were traced to Iran and Qatar, key states that supported Hamas in the conflict against Israel.[24]

Given Israel's security environment and the increase in advanced cyber attacks, it has since developed a sophisticated cyber defence strategy that encompasses multi-faceted dimensions of cyber defence. A Policy Report on Israel's evolving cyber defence strategy states that:

> *"The IDF's strategy is... [focused on] developing unique interdisciplinary methodologies in a multidisciplinary national 'cyber-ecosystem' that integrates national research laboratories, military intelligence units, C4I organisations, the National Cyber Bureau, and start-up firms and entrepreneurs. In doing so, Israel is developing a "national cyber defence envelope" – a multi-layered cyber defence strategy leveraging automated computerised systems and highly-trained personnel that proactively combine intelligence, early warning, passive and active defence, and offensive capabilities across civil-military domains."*[25]

While there are no specific details and information about the IDF's cyber capabilities and operations from open sources, it is clear that much emphasis is placed by the IDF on active cyber defence, even to the extent of overtly mentioning offensive cyber capabilities in their menu of defences. In June 2015, the IDF announced that it would establish a new cyber command to lead all operational cyber activities, and it would be the fifth of such a branch directly subordinate to the Chief of Staff, other than the four existing Army, Air Force, Navy and Intelligence branches.[26] The establishment of this new organisation reflects the increasing importance of providing dedicated focus on integrating passive and active cyber capabilities in order to put in place a multi-layered cyber defence envelope.

The broad review of the US and Israel's national-level cyber defence strategies highlight that these states have embraced "a collaborative triptych of approaches to cyber security."[27] According to Robert Dewar, these approaches are not purely passive or active cyber defences; instead, a clearer categorisation of these measures would be to define them as fortified, resilient and active cyber defence.[28] These three pillars of cyber defence concept complement one another in providing a multi-layered and comprehensive cyber security approach. When combined, these strategies are able to address cyber threats ranging from low-level attacks (such as virus and DDoS attacks) to advanced cyber threats in the form of the next *Stuxne*t.

A COMPREHENSIVE CYBER DEFENCE STRATEGY FOR THE RSAF

In defining how the concepts of fortified, resilient and active cyber defences could be applied, we can draw parallels to key RSAF concepts and measures to identify the essential building blocks of an effective cyber defence framework.

As shown in *Figure 3*, passive and active cyber defence capabilities can be broadly categorised according to the nature of actions taken to defend against cyber threats. On one end of the continuum, there are passive defence mechanisms that serve to strengthen and fortify critical networks and infrastructures. In the middle of the continuum are cyber defence concepts that confer network resilience through responsive, adaptive, and occasionally deceptive actions to assure continued operations despite on-going attacks. At the most active end of cyber defence measures are proactive and active cyber defence operations that rely on well-researched threat intelligence.[29]

Fortification: 'Hardening' Our Infrastructure

Fortification of critical networks and infrastructures serves to reduce chances of a successful malicious attacks by preventing malicious access. This can take the form of installation of firewalls, encryptions and anti-virus software into operational systems and the supporting infrastructure, such as routers, network switches and computer software. Such forms of cyber

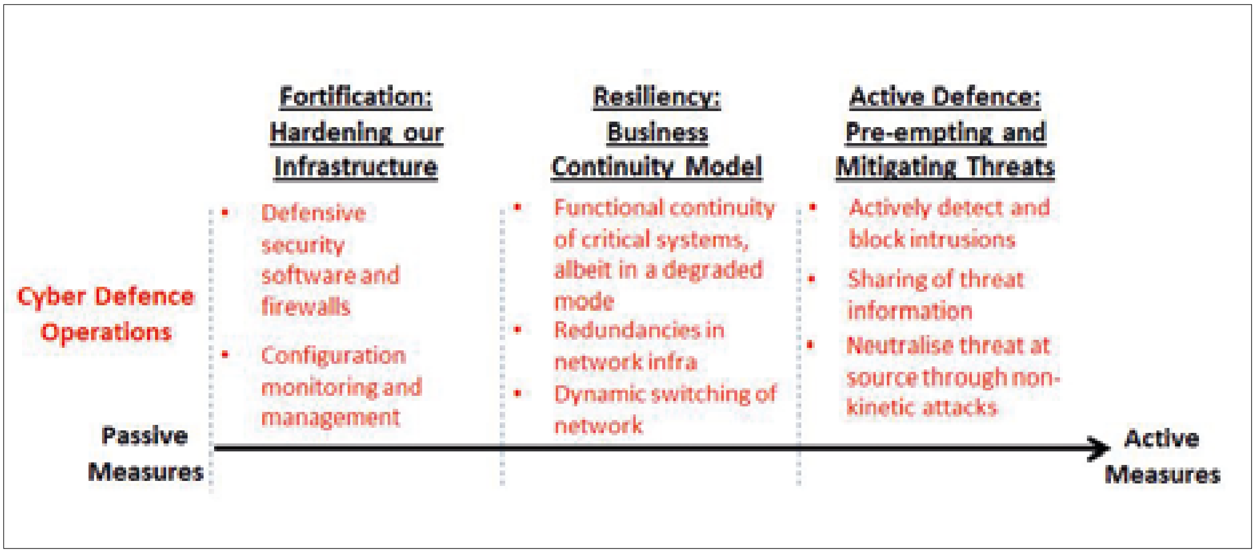

Fortification: Hardening our Infrastructure
Resiliency: Business Continuity Model
Active Defence: Pre-empting and Mitigating Threats
Cyber Defence Operations
• Defensive security software and firewalls
• Configuration monitoring and management
• Functional continuity of critical systems, albeit in a degraded mode
• Redundancies in network infra
• Dynamic switching of network
• Actively detect and block intrusions
• Sharing of threat information
• Neutralise threat at source through non-kinetic attacks
Passive Measures
Active Measures

Figure 3: Cyber defence concepts explained using Air Force Analogies

defence are akin to the hardening of our critical infrastructure against enemy air strikes, which is needed to protect our assets against external attacks.

Not surprisingly, many established militaries have recognised fortified cyber defence as one of the foundational pillars of cyber defence and have taken quick and extensive steps to establish cyber defensive perimeters to systematically secure communications and information networks.[30] Similar to the hardening of physical infrastructure, the implementation of cyber fortification across the entire organisation's network and computer systems can be costly and time-consuming. For example, a Task Force Report by the US Defence Science Board projected the investment cost for protecting the DoD's systems against low and mid-tier threats to be around US$50M to US$100M per year and would take around 18 months to complete.[31]

At the most active end of cyber defence measures are proactive and active cyber defence operations that rely on well-researched threat intelligence.

Fortification measures, though effective against novices and sporadic attacks, would eventually be defeated by determined and well-resourced attackers, especially when sophisticated attack techniques are employed to create new vulnerabilities in the systems, instead of merely exploiting existing security gaps. In addition, human errors, ignorance, wilful deviations from security protocols can often become the weakest link and provide determined attackers the much awaited opportunity to infiltrate our system to wreak havoc.[32] Overly-focusing our investments in fortification efforts will eventually yield diminishing returns in cyber defence effectiveness. Hence, we should adopt a balanced and pragmatic strategy by complementing our fortification efforts with a concept of cyber resilience, which would ensure sustained operational effectiveness in the face of cyber attacks.

Resiliency: Developing A Business Continuity Model

Resilient Cyber Defence is essentially about developing a business continuity model that focuses on survivability and functional continuity of the identified critical systems. In the event of a malicious attack or natural disruption to the system, a resilient cyber network will be able to prioritise its resources to ensure the provision of its primary service, albeit in a degraded mode.[33] For example, a power plant with a resilient cyber system encountering a cyber-breach will only suffer minor disruptions and still be able to produce a minimal but sufficient electrical output. Drawing a parallel to our Air Force, this is similar to our emphasis on robust air power generation through our investment in rapid runway repair capabilities to ensure a quick recovery of our air campaign after enemy air raids.

Embracing this concept of resilience is especially critical for the RSAF as it can provide the assurance of operational continuity in our centralised command and control of air operations by mitigating the impact of a successful cyber breach on the progress of air campaign. Simply put, building a resilient cyber system allows our commanders to continue with their orchestration of the air campaign with little or no degradation in their situational awareness or hindrance to their abilities in directing dispersed elements in the field and in the sky, even when a malicious cyber attack has taken place.

As part of this concept, it will be essential to establish a framework for the identification of critical systems that must incorporate high resiliency features, in addition to the systemic passive defence measures. In the operations phase, a highly competent crew of network experts must be able to accurately analyse and contain the operational impact of a successful cyber attack on the overall RSAF campaign.

This resilience concept proposes that in addition to providing agile and adaptive Command and Control, dynamic switching of network configuration reduces the chances of a successful 'target reconnaissance' by the adversary. In addition, incorporating decoys in the unused regions of our network space could further obfuscate any reconnaissance effort, thereby increasing the amount of resources required of the enemy for a successful cyber attack.[34] The incorporation of decoys also provides data points and insights into any malicious activities, which can be used to substantiate intelligence gathering efforts. Such intelligence will be crucial for beefing up cyber defence measures, and can also form the basis of more active cyber defence operations, as explained in succeeding paragraphs. To this end, the RSAF can closely partner the defence technology community to develop and incorporate such techniques into our existing network infrastructures.

Active Defence: Pre-Empting and Mitigating Threats

While fortified and resilient cyber defence are considered passive approaches that focus on defending our networks and making them more resilient to attacks, active cyber defence involves a broad range of proactive measures to mitigate threats. The fundamental concept of active cyber defence is to actively detect and mitigate the threat before it inflicts damage on its intended target.

Proactive actions can be taken to neutralise or mitigate threats in different ways. According to Dorothy Dennings, active cyber defence actions can be classified into four categories: sharing, collecting, blocking and pre-emptive.[35] First, sharing 'refers to actions that distribute threat information' to other parties so as to mitigate the effectiveness of the threat. In air defence operations, such actions are analogous to sharing information on missile or aircraft threats to other SAF entities outside our network so that we can collectively counter the threat.

The second category is collecting, which is to "take actions to acquire more information about the threat."[36] This would include measures such as deploying additional sensors to detect intrusions, or deploy 'white worms' that are similar to viruses that can search, collect information and subsequently destroy malicious software.[37] In air defence lingo, this would be analogous to mounting additional surveillance radars to a heightened alert state or sending out fighter aircraft to intercept, identify potential air threats and subsequently shoot these threats down.

The third category is blocking, which comprises actions taken to block suspicious software or activities from suspected hostile IP addresses. It would also include identifying, analysing and blocking software or traffic that displays abnormal behaviours or match specific threat signatures.[38] Such actions are akin to the Israeli's Iron Dome concept, where incoming aircraft or missile threats are shot down or prevented from hitting their intended targets.

The fourth category is pre-emptive actions, which is to 'neutralise or eliminate a source used in the attacks'.[39] For example, it could involve hacking back the computer that is initiating the attack, or it could involve shutting down hostile servers for a botnet. Other times, when intelligence gathering has provided sufficient evidence of pending malicious activities from an external source, it could mean a pre-emptive cyber attack to take down the server or computer even before it could launch an attack. This may neutralise or eliminate the cyber threat.

OUR PEOPLE: THE CRUCIAL LINK

Even as we continue to invest in technologies that fortify our networks, provide better resilience against malicious cyber attacks and develop active defence capabilities to mitigate threats, it is important to turn to our people—the crucial link in the larger cyber defence architecture. Much can be done to shape cultures and mindsets, train operational instincts and to be in tune with the realities of today's cyber operational environment and the opportunities and challenges that accompany it.

Even as we continue to invest in technologies that fortify our networks, provide better resilience against malicious cyber attacks and develop active defence capabilities to mitigate threats, it is important to turn to our people—the crucial link in the larger cyber defence architecture.

Our RSAF warfighters must recognise that the cyber space domain is as real and important as the air, land and sea domains. We must understand the limitations and fundamental assumptions of operating in the cyber space domain. For example, we must ensure that our RSAF warfighters are cognisant that in the contested cyber space environment, the intent and attribution of cyber threats may be difficult to ascertain. In addition, we can fortify or secure our networks, but adversaries will try to probe and they need only to be successful once to create an impact on our operations.[40] Moreover, we should see our networks not simply as support systems, but rather, to treat the entire network itself as a strategic weapon system.[41]

Shaping the organisational culture and our people's mindsets to align with this frame of thought is important, so that our warfighters see themselves as each being crucial elements and gatekeepers of a strategic weapon system. This is analogous to the RSAF Safety Culture, which was painstakingly built over the years to ensure that our personnel are imbued with a 'Safety First' mindset to enhance our operational effectiveness. Just as Safety is a personal, command and organisational responsibility, cyber security is the responsibility of each RSAF warfighter and at every level. A single point of failure has the potential to create devastating effects to the entire cyber network. We will need to safeguard our cyber space 24/7, just as how we constantly safeguard our airspace.

We can also do more to train our people to have the operational instincts to be effective in the cyber domain. For example, the United States Air Force (USAF) is incorporating the cyber domain at the tactical and operational levels at the Red Flag series of exercises to reflect the growing importance of cyber operations on the battlefield.[42] The USAF cyber teams that participated in the exercises are able to get hands-on training while exercising a variety of their cyber capabilities. They will target the adversary and their infrastructures to degrade their capabilities, as well as simultaneously defend critical infrastructures and networks.[43] The RSAF should similarly consider incorporating cyber elements as a staple in our key exercises. This not only hones our warfighters' operational instincts in the cyber domain, but also reflects the RSAF's organisational emphasis on the cyber space domain.

CONCLUSION

As the RSAF continues to modernise and advance technologically, our systems will increasingly depend on networks and System-of-Systems (SoS) capabilities to shorten the Observe, Orient, Decide and Act (OODA) loop to deliver airpower more decisively. Our networks will also be linked to other networks in the Army and Navy for better synergy in the air, land and sea campaigns.

However, just as technology and networks are enablers for enhanced Command and Control (C2) for the RSAF, they are also vulnerable to cyber attacks. With the increasing use of cyberspace as the fifth domain in military warfare, it is of paramount importance for the RSAF to continue to build up and strengthen our cyber defence capabilities, processes and competencies in accordance with a comprehensive cyber defence strategy.

While cyber defence strategies comprising fortified, resilient and active cyber defence are not new concepts, the methods and means to implement these strategies are continuously evolving in tandem with the sophistication of cyber threats. The RSAF and Singapore Armed Forces (SAF) will need to partner with Singapore's defence technology community to develop revolutionary innovations that can enhance Singapore's national security. Most importantly, we also need to shape our organisational culture and train our people to ensure that we are always vigilant against cyber attacks that may be employed as part of hybrid warfare.

ENDNOTES

1. Ng Eng Hen, Speech by Minister for Defence Dr Ng Eng Hen at the Committee of Supply Debate 2016, posted 8 Apr 2016, http://www.mindef.gov.sg/content/imindef/press_room/official_releases.sp.html.

2. Frank .G Hoffman, “Hybrid Warfare and Challenges,” Joint Force Quarterly 52 (October 2009): 34-39, http://smallwarsjournal.com/documents/jfqhoffman.pdf.

3. Steven Bucci, “The Confluence of Cyber Crime and Terrorism,” Lecture #1123 on National Security and Defence, The Heritage Foundation, last modified June 12, 2009, http://www.heritage.org/research/lecture/the-confluence-of-cyber-crime-and-terrorism.

4. For a brief introduction on the early years of cyber threats, see Andrew F. Krepinevich, Cyber Warfare: A Nuclear ‘Option’? Center for Strategic and Budgetary Assessments (2012), 41-45.

5. For more information on how criminal groups use malware to commit cyber-crime, see Joseph Menn, Fatal System Error: The Hunt for the New Crime Lords who are Bringing Down the Internet, 1st ed. (New York: Public Affairs, 2010).

6. Alexander Klimburg, “Mobilising Cyber Power,” Survival 53 (2011): 49, as referenced in “A Walk on the Dark Side,” The Economist, 2007, accessed June 1, 2012, http://www.economist.com/node/972376.

7. Steven Herzog, “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses,” Journal of Strategic Security 4, no.2 (2011): 49-60, http://dx.doi.org/10.5038/1944-0472.4.2.3.

8. David Hollis, “Cyberwar Case Study: Georgia 2008,” Small Wars Journal, posted January 6, 2011, http://smallwarsjournal.com/printpdf/10080.

9. Michael Raska, “Confronting Cybersecurity Challenges: Israel’s Evolving Cyber Defence Strategy,” S. Rajaratnam School of International Studies, Nanyang Technological University (January 2015): 6, https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf.

10. Krepinevich, Fatal System Error, 5-6.

11. Ibid., 3.

12. Michael B. Kelley, “The Stuxnet Attack on Iran's Nuclear Plant was 'Far More Dangerous' than Previously Thought,” Business Insider, November 20, 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T&r=US&IR=T.

13. Lee Ferran, Alexander Marquardt and Colleen Curry, “Flame Cyber Attack: Israel Behind Largest Cyber Spy Weapon Ever?” ABC News, May 29, 2012, http://abcnews.go.com/Blotter/flame-cyber-attack-israel-largest-spy-weapon/story?id=16449339.

14. Nicholas Falliere, L. Omurchu and E Chien, “W32. Duqu: The precursor to the next Stuxnet,” Symantec Security Response (November 2011), available at www.usenix.org/conference/leet12/workshop-program/presentation/chien.

15. The definition of Advanced Persistent Threat (APT) is taken from National Institute of Standards and Technology (NIST). See NIST, Managing Information Security Risk: Organization, Mission, and Information System View. SP 800-39, 2011, quoted in Ping Chen, Lieven Desmet and Christophe Huygens, “A Study on Advanced Persistent Threats,” in IFIP International Conference on Communications and Multimedia Security (2014): 64, DOI: 10.10071978-3-602-44885-4_5.

16. Irving Lachow, Active Cyber Defence: A Framework for Policymakers, Policy Brief (Washington, DC: Center for North American Security, February 22, 2013): 2, http://www.cnas.org/publications/policy-briefs/active-cyber-defence-a-framework-for-policymakers#.V9f93_CGOM8.

17. Ibid.

18. Pierluigi Paganini, “Operation Dust Storm, Hackers Target Japanese Critical Infrastructure,” Security Affairs, February 24, 2016, http://securityaffairs.co/wordpress/44749/cyber-crime/operation-dust-storm.html.

19. William J. Lynn, “Defining a New Domain: The Pentagon’s Cyberstrategy,” Foreign Affairs 89,no. 5, (September/October 2010): 98, http://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

20. As defined by the US Department of Defence in Department of Defence Strategy for Operations in Cyberspace (July 2011), 7. See also Lachow, Active Cyber Defence, 2.

21. Lynn, “Defining a New Domain,” 98.

22. Ibid.

23. Raska, “Confronting Cybersecurity Challenges,” 5.

24. Lappin Yaakov, “Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source Says,” The Jerusalem Post, August 18, 2014, http://www.jpost.com/Arab-Israeli-Conflict/Iran-attempted-large-scale-attack-on-Israel-senior-security-source-says-371339.

25. Raska, “Confronting Cybersecurity Challenges,” 5.

26. Meir Elran and Gabi Siboni, “Establishing an IDF Cyber Command,” The Institute for National Security Studies, Insight No. 719, July 8 2015, http://www.inss.org.il/index.aspx?id=4538&articleid=10007.

27. Robert S. Dewar, “The 'Triptych of Cyber Security': A Classification of Active Cyber Defence,” in Cyber Conflict (CyCon 2014): 8, http://ieeexplore.ieee.org/document/6916392.

28. Ibid.

29. The spectrum of measures was adapted from Robert Lee’s sliding scale of cyber security. See Robert M. Lee, The Sliding Scale of Cyber Security, SANS Analyst Whitepaper (August 2015), http://www.sans.org: https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240.

30. Carmen-Cristina Cirlig, Cyber Defence in the EU: Preparing for Cyber Warfare? European Parliament Think Tank, http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.

31. James R. Gosler and Lewis Von Thaer, Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, (Washington DC: Department of Defence, Defence Science Board, 2013): 11-12.

32. Joanna Belbey, "The Weakest Link in Cybersecurity," Forbes Online, February 27, 2015, http://www.forbes.com/sites/joannabelbey/2015/02/27/the-weakest-link-in-cybersecurity/#6ee205137410.

33. Dewar, "'Triptych of Cyber Security'," 15-16.

34. Keith A. Repik, Defeating Adversary Network Intelligence Efforts with Active Cyber Defence Techniques, (Ohio: Department of Air Force Air University, Air Force Institute of Technology, 2008): 46

35. Dorothy E. Denning, "Framework and Principles for Active Cyber Defence," Computers & Security 40 (2014): 4,http://faculty.nps.edu/dedennin/publications/Framework%20and%20Principles%20for%20 Cyber%20Defence%20-%2011Dec2013.pdf.

36. Ibid.

37. Dewar, "'Triptych of Cyber Security'," 9.

38. Denning, Framework and Principles for Active Cyber Defence, 3-4.

39 Ibid, 5.

40. Henry Kenyon, "Air Force Embraces New Mindset for Cyber Warfare," National Defence Industrial Association, January 31, 2011, https://defencesystems.com/articles/2011/01/31/air-force-cyber-command-ready-for-operations.aspx.

41. Ibid.

42. Joey Cheng, "Sign of the Times: Cyber's Bigger Role in Air Force's Red Flag," Defence Systems, October 3, 2014, https://defencesystems.com/articles/2014/10/03/air-force-red-flag-cyber-domain.aspx.

43. Ibid.

LTC Anthony Wong is a fighter pilot by vocation and currently serving as a Branch Head. A recipient of the SAF Academic Scholarship (Military), LTC Wong graduated from the Australian Defence Force Academy and holds a Bachelor of Science in Chemistry from the University of New South Wales. He was also a recipient of the SAF Post graduate Award and holds a Master of Arts in Security Studies from the Naval Postgraduate School.

MAJ Christopher Eng is an AWO (GBAD) by vocation and is currently Head of New Media and Public Relations in Air Operations Department, Air Force Information Centre. He graduated from NUS with a Degree in Mechanical Engineering (Aeronautical) (Honours). He was previously Officer Commanding (OC) of 163 SQN.

CPT Ronald Loh Ming Yao is a helicopter pilot by vocation, and is currently a Staff Officer in Joint Operations Department. CPT Loh was a recipient of the SAF Merit Scholarship in 2009. He graduated from the University of Warwick with a Bachelors of Science in Economics, Politics, and International Studies (Hons, 1st Class), and subsequently from Columbia University with a Masters of Arts in Political Science.

CPT Jeffrey Ng is currently serving as an OC in 119 SQN, UAV Command. He is a UAV Pilot by vocation, and is a Command Pilot of the Heron 1 UAV. A recipient of the SAF Merit Scholarship in 2008, he graduated from University College London with a Bachelors of Science in Psychology with Honours in 2011, and subsequently from the University of Edinburgh with a Masters of Science in Performance Psychology.